MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2016/2017

BSE3024 – SECURITY & E–PAYMENT SYSTEM

(All sections / Groups)

25 FEBRUARY 2017
2.30 p.m – 4.30 p.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 4 pages with 4 Questions only.
2. Attempt **ALL** questions. Marks are shown at the end of each question
3. Please print all your answers in the Answer Booklet provided.

ESSAY QUESTIONS (100 Marks)

There are TWO sections. Section A is case study. Section B is essay questions. Answer ALL questions in BOTH sections.

Section A: Case Study

Question 1

Hidden Dangers Lurking in E-Commerce:
Reducing Fraud with the Right SSL Certificate

Shopping online has now become almost second nature to most of us, but where did it all start, and what enabled it to grow to the levels that we see today? Reportedly, it was back in 1994, with the first known web purchase being a pepperoni pizza with mushrooms and extra cheese from Pizza Hut. When that first pizza was ordered – and, a year later, when online retail giant Amazon sold its first book (Douglas Hofstadter's 'Fluid Concepts & Creative Analogies: Computer Models of the Fundamental Mechanisms of Thought'), it ushered in a torrent of activity.

Two decades later, global e-commerce sales for 2013 have been calculated at upwards of $1.2 trillion. What facilitated this tectonic shift in our shopping habits? Trust. Trust in who we were shopping with, and trust that the purchase information we provided would be secured. Because as ever, where there is money there will always be criminals - eager to take advantage of the burgeoning opportunity. But if trust is the grease that lubricated the online marketplace, what is the technical basis for that trust? The answer is in part solved with Secure Sockets Layer (SSL), and more specifically, digital certificates - a reliable technology which has worked well for decades, and can continue to do so. But for this to happen, it has to be deployed responsibly. Put simply, not all certificates are created equal – and today, some ingenious criminals have found a way to corrupt the very system that was designed to stop them. As a result, we need to make sure that certificates are matched to their uses and that when people send their personal and financial information across the internet they can have confidence that the recipient is not a criminal.

In fact, research from Norton estimates the global price tag of consumer cybercrime now topping some US$113 billion annually4 which is enough to host the 2012 London Olympics nearly 10 times over. The cost per cybercrime victim has shot up to USD$298: a 50% increase over 2012. In terms of the number of victims of such attacks, that's 378 million per year – averaging 1 million plus per day.

Looking at the way we all interact online, it's important to understand the threat landscape and help the industry take the required action. The fact is that e-commerce can prove to be extremely compulsive – buy something now! With cost, time until delivery, and returns policy often highest up the agenda, security is typically an afterthought at most. It's no wonder that the cyber criminals have moved in en masse, lured by the easy pickings

and riches to be had. And it's this movement that makes security and particularly the use of security online more important today than ever before.

Ideally what the industry needs to do is ensure that if consumers are spending money online, they should be able to trust the site they are shopping on. To do this the industry needs to make a step change to the type of SSL certificates that help make e-commerce trustworthy.

Source: Semantec (UK) Limited. 2015. Hidden Dangers Lurking in E-Commerce - Reducing Fraud with the Right SSL Certificate. White paper. Pg. 1-15. Accessed on 15 Dec 2016 from https://www.symantec-wss.com/campaigns/16493/assets/16493-Hidden-Dangers-Lurking-in-E-Commerce-UK.pdf

Answer the following questions:

a. Why online shopping is vulnerable? In an E-commerce environment, indicate the vulnerable points. Use a diagram to support your answer. (10 marks)

b. Define Secure Socket Layer (SSL). How does it work? Explain your answer with a diagram. (11 marks)

c. Discuss the following statement:

"Ideally what the industry needs to do is ensure that if consumers are spending money online, they should be able to trust the site they are shopping on."
(10 marks)

d. Discuss any THREE (3) elements of a good security policy that every e-commerce business should have. (9 marks)

(Total: 40 marks)

Section B: Essay Questions

Question 2

a. 11street is Malaysia's latest one stop online shopping mall that connects customers to variety of products in a trustworthy and secure environment for buyers and sellers. You are hired by 11street to develop an E-commerce security plan. Outline the FIVE (5) stages and explain the requirements. (10 marks)

b. Define Single Symmetric Encryption Method. Draw a diagram to support your answer. (10 marks)

(Total: 20 marks)

Question 3

a. Discuss TWO (2) payment security measures in order to expand online sales. (10 marks)

b. Discuss FOUR (4) security risk with credit card payment online. (10 marks)

(Total: 20 marks)

Question 4

On Friday, October 21, 2016, a series of IoT DDoS (Internet of Things Distributed Denial of Service) attacks caused widespread disruption of legitimate internet activity in the US. Describe what is IoT DDoS attack. Discuss security measures for E-Commerce from IoT DDoS.

(Total: 20 marks)

End of Page